VERKKOPANKKILINKKI

Linkki verkkopankista pankin ulkopuoliseen palveluun

Palvelun kuvaus ja palveluntarjoajan ohje v 2.0

FINANSSIALA

FINANSSIALA

Sisällysluettelo

Itämerenkatu 11-13
00180 Helsinki
Puh: +358 20 793 4200
Fax: +358 20 793 4202
etunimi.sukunimi@finanssiala.fi
www.finanssiala.fi
Facebook.com/finanssiala
Twitter.com/finanssiala

FINANSSIALA

Versiopäivitys

26.5.2008	Versio 1.3: edellinen käytössä ollut versio
29.2.2024	Versio 2.0: tietoturvapäivityksiä kuvaukseen, ajantasaistettu tekstiosiot

1 Verkkopankkilinkin kuvaus

Verkkopankkilinkki tarjoaa yrityksille mahdollisuuden vähentää paperilla toimitettavien dokumenttien tulostusta ja jakelua. Verkkopankkilinkin avulla kuluttaja-asiakas voi siirtyä pankin sähköisestä palvelusta tunnistettuna ulkoisen palveluntarjoajan palveluun.

Verkkopankkilinkki on pankkien yhteisesti standardoima. Palveluntarjoaja sopii linkin käyttöönotosta kaikkien niiden pankkien kanssa, joiden verkkopankkia käyttäville asiakkaille linkki halutaan tarjota.

1.1 Yleiskuvaus

Verkkopankkilinkki muodostetaan verkkopankissa olevasta tapahtumasta, johon näin voidaan antaa lisätietoja tai tarkempi erittely pankin ulkopuolisessa palvelussa.

Linkki yhdistää verkkopankkia käyttävän asiakkaan palvelun tarjoajan esilläpitopalveluun Internetissä. Linkki sisältää tiedot, joiden avulla palveluntarjoaja voi kohdistaa linkin oikeaan tapahtumaan.

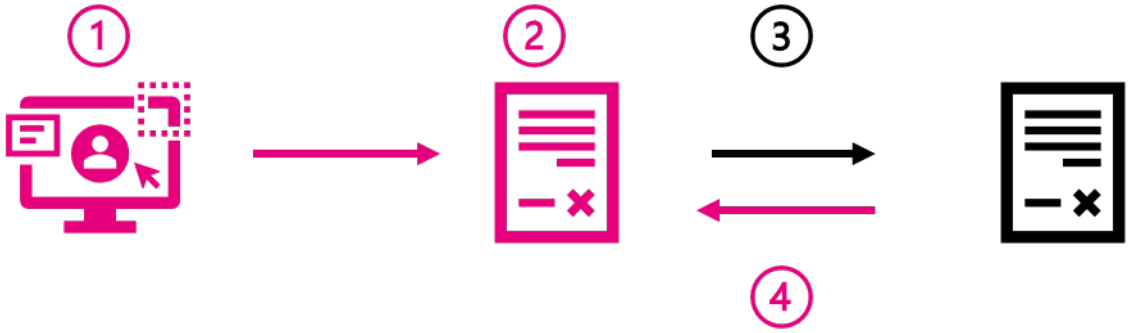
Tietoliikenne on salattua ja välitettävien tietojen eheys turvattu tarkisteella.

1.2 Soveltaminen

Yleisin käyttötapaus on kuluttajan e-laskutuksessa. Kuluttaja haluaa katsoa tarkempia tietoja pankin sähköiseen palveluun saamastaan e-laskusta. Tällöin hän siirtyy e-laskussa olevasta linkistä laskuttajan palveluntarjoajan laskujen esilläpitoarkistoon.

Toinen yleinen käyttötapaus on siirtyminen pankin palvelusta katsomaan omaa palkkalaskelmaansa verkkopalkkaoperaattorin palveluun.

2 Verkkopankkilinkin toiminnallinen kuvaus



Tässä kuvauksessa käytetään esimerkkinä e-laskun esilläpitoarkistoon siirtymistä. Sama toimintalogiikka käy myös verkkopalkkaan.

1. Pankin asiakas kirjoittautuu pankin sähköiseen palveluun (esim. verkkopankki, mobiilisovellus) ja haluaa tarkastella saamaansa e-laskua
2. E-laskussa voi olla verkkopankkilinkki.
3. Linkin käyttö yhdistää asiakkaan palveluntarjoajan Internet-palveluun (esilläpitoarkisto) ja siellä laskusta esitettyihin tietoihin, jotka voidaan esittää esim. erillisenä selainikkunana.
4. Kun verkkopankin asiakas lopettaa palveluntarjoajan Internet-palvelun käytön (esim. sulkemalla selainikkunan), hän palautuu pankin sähköiseen palveluun ja voi hyväksyä esimerkiksi hyväksyä laskun.

Jos verkkopankin timeout-aika on täyttynyt asiakkaan asioidessa palveluntarjoajan verkkosivuilla, täytyy asiakkaan kirjoittautua uudelleen pankin palveluun.

3 Verkkopankkilinkin käyttöönotto

Palveluntarjoaja sopii verkkopankkilinkin käyttöönotosta kunkin pankin kanssa erikseen. Palvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä. Palveluntarjoajan tiedot rekisteröidään kussakin pankissa ja palveluntarjoaja ilmoittaa kullekin pankille erikseen, kun hänen sopimustietoihinsa tulee muutoksia.

Pankki toimittaa palveluntarjoajalle sopimuksen teon jälkeen palvelussa käytettävän tunnuksen ja tarkisteavaimen. Tiedot toimitetaan palveluntarjoajalle pankkikohtaisella menettelyllä joko sähköisessä muodossa tai paperitulosteena. Toimitettavat tiedot on suojattu kuljetuksen aikana siten, että vastaanottaja voi havaita, jos toimituksen suojakuori on avattu kuljetuksen aikana.

Testausmenettelyt ovat pankkikohtaisia ja niistä löytyy lisää tietoa pankkien omista palvelukuvauksista.

4 Turvallisuus

Verkkopankin ja esilläpitopalvelun välisessä tietoliikenteessä käytetään TLS-salausprotokollaa, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Linkin kohteena olevien palvelun tarjoajan tietojen tulee myös olla TLS-suojattuja. TLS-protokollasta tulee käyttää vähintään versiota 1.2.

Pankki tunnistaa verkkopankkiasiakkaansa. Verkkopankkilinkissä pankin esilläpitopalvelulle välittämät tiedot perustuvat e-laskun ja verkkopankkiasiakkaan tietoihin. Linkin tiedot on lisäksi suojattu tiedon eheyden turvaavalla tarkisteella, joten linkkiä käyttävä verkkopankin asiakas ei voi muuttaa tietoja palveluntarjoajan sitä havaitsematta.

5 Verkkopankkilinkin parametrit

Merkkijono muodostuu parametrikenttien sisällöistä ja &-merkeistä kenttien välissä. Kentän nimi yhdistetään arvoon =-merkillä. Merkkijonon loppuun liitetään salainen avaintieto ja &-merkki. Merkkijonot eivät sisällä tyhjemerkkejä.

Kaikki merkkijonot on koodattu käyttäen koodistoa ISO 8859-1, ellei muuta ole erikseen määritelty.

URL	Pituus	Kuvaus
https://www.yritys.fi/aaaa/bbbbbb/cccccccc	enintään 2048 merkkiä	- protokolla, TLS-salaus - palvelimen nimi - esilläpitopalvelun nimi ko. palvelimella

Kentän nimi	Arvo	Pituus	Kuvaus
VERSION	0001 tai 0020	4 numeroa	Linkin versionumero (0020 = v. 2024 päivitetty versio). Jokin määritellyistä arvoista.

PMTREFNB		enintään 96 merkkiä	Linkin kohteena olevan tapahtuman yksilöintitieto - verkkopalkassa palkansaajan henkilötunnus (123456-789X) salattuna - salattavan datan selkokielisen representaation pituus max. 64 merkkiä - salatun datan salatun representaation pituus max. 96 merkkiä - kuluttajan e-laskussa pituus max. 60 merkkiä - laskuun liittyvän lisätiedon arkistointitunnus (esimerkiksi laskun viite, laskuttaja syöttää tiedon Finvoice-verkkolaskulle kenttään InvoiceUrlText) - PMTREFNB:iä ei kuluttajan e-laskussa salata. Mikäli PMTREFNB-kenttä on salattu, linkin MAC-tarkisteen laskentaan käytetään PMTREFNB-kentän salattua arvoa. Katso lisäselvitys parametrin salauksesta 5.2

RCVID		enintään 20 merkkiä	Laskuttajan tai palkanmaksajan tunnus pankissa. Kuluttajan e-laskussa ei käytössä.
TIMESTMP	VVVV-KK-PP-HHMMSS+HH tai VVVV-KK-PPHHMMSS%2BHH	22 tai 24 merkkiä	Linkin muodostushetki, aikavyöhykkeen esitysmuoto voi olla pankista riippuen joko +HH tai %2BHH, +02 = %2B02 = normaaliaika Suomessa +03 = %2B03 = kesäaika Suomessa. Katso lisäselvitys parametrin käytöstä 5.1
KEYVERS		4 numeroa	MAC-avaimen versio. Sisältää arvon välillä 0000-9999. Katso lisäselvitys parametrin käytöstä 5.4

ALG	0003 = SHA-256 0004 = SHA-512	4 numeroa	MAC-avaimen laskenta-algoritmien SHA-256 tai SHA-512. Jokin määritellyistä arvoista.
LANGCODE	1 = suomi 2 = ruotsi 3 = englanti	1 numero	Asiakkaan kielikoodi verkkopankissa. Jokin määritellyistä arvoista.
SESSIONID		enintään 20 merkkiä	Pankin määrittämä istuntotunniste lokitettavaksi mahd. selvitystilanteita varten.
SENDID		enintään 20 merkkiä	Linkin muodostajan tunnus. Kuluttajan e-laskun sisältämässä pankin muodostamassa linkissä SENDID-kentässä on linkin muodostaneen pankin BIC-osoite.
MAC			Linkin MAC-tarkiste. Kaikista käytössä olevista parametreista laskettu tarkiste. Linkin muodostava palvelin laskee parametritiedoista tarkisteen arvon. MAC-tarkiste sijoitetaan suuraakkosin esitetyssä heksadesimaalimuodossa parametrikentän MAC-arvoksi. Linkki tulee hylätä, mikäli sen sisältämä MAC tarkiste ei vastaa parametrien perusteella laskettua tarkistearvoa.
STATUS	Prod = tuotantolinkki Test = testilinkki	4 merkkiä	Linkin tila. Jokin määritellyistä arvoista.
Valinnaiset tiedot:			
PMTORIG	1 = kuluttajan e-lasku 2 = verkkopalkka	1 numero	Maksun syöttötapa. Jokin määritellyistä arvoista.
ENCALG	0001 = AES-256-CBC	4 numeroa	Salausalgoritmi. Jokin määritellyistä arvoista.

ENCKEYVER	0001 jne.	4 numeroa	Salausavaimen versio. Sisältää arvon välillä 0000-9999. Katso lisäselvitys parametrin käytöstä 5.5
USERMAC		32 merkkiä	Maksajan henkilötunnuksesta muodostettu tarkiste. Katso lisäselvitys parametrin käytöstä 5.3

5.1 Lisäselvitys TIMESTMP-parametrin käytöstä

Vastaanottavan palvelun on tarkastettava, ettei linkkiä käytetä ennen kuin aikaisintaan 15 minuuttia ennen TIMESTMP-aikaleiman hetkeä tai 15 minuuttia TIMESTMP-aikaleiman hetkeä myöhemmin. Tarkastus tehdään vertaamalla TIMESTMP- ja PMTREFNB-parametrien arvoja. Lisäksi linkki voidaan käyttää vain kerran.

5.2 Lisäselvitys PMTREFNB-kentän salauksesta

AESia käytettäessä käytetään CBC-menetelmää, jossa käytetään 16 tavun (128 bitin) pituista Initialization vector (IV) -parametria. IV-parametri ei saa olla ennakoitavissa, eli sen tulee olla satunnaisesti tai pseudosatunnaisesti generoitu. IV-parametria ei saa koskaan käyttää uudelleen. (Soveltamisohje: käytetyistä IV-parametreista ei tarvitse pitää kirjaa, mikäli käytetyssä pseudosatunnaislukugeneraattorissa ei ole tunnettuja haavoittuvuuksia. IV-parametrin mahdollisten arvojen määrä on riittävän suuri, että mahdollisten satunnaisten törmäysten todennäköisyys IV-parametrien generoinnissa voidaan katsoa merkityksettömän pieneksi.)

Avaimen pituus on 256 bittiä.

Salattavan selkokielisen lohkon merkkikoodisto on ISO 8859-1. Salattava selkokielinen lohko on 16 merkkiä pitkä. Lohkon alussa (vasemmassa reunassa) on henkilötunnus (123456-789X). Loppuosa lohkosta on täytetty tyhjemerkeillä. Lohko ei saa sisältää merkkejä ’&’ tai ’=’.

Salauksen tuloksena syntyvä salatekstilohko sisältää lohkon alussa (vasemmassa reunassa) 16 tavun mittaisen IV-parametrin, joka on saman mittainen kuin yksi AES-lohko, standardin mukaisesti. Tätä seuraa välittömästi 16 tavun mittainen varsinainen salateksti (yksi 16 tavun mittainen AES-lohko). Koko salatekstilohkon pituus on siis 32 tavua. Koko salatekstilohko - IV ja salateksti molemmat mukaan lukien - esitetään heksadesimaalisessa esitysmuodossa, jossa A-F esitetään suuraakkosilla. Tämän heksadesimaalisen esitystavan pituus on 64 merkkiä.

Mikäli PMTREFNB-kenttä on salattu, linkin MAC-tarkisteen laskentaan käytetään PMTREFNB-kentän salattua arvoa heksadesimaalisessa esitysmuodossa.

5.2.1 Esimerkki PMTREFNB-kentän salatun arvon laskemisesta

Salattava selkokielinen syöte:
”010101-999X ”

Koko salattava selkokokielinen lohko heksadesimaalimuodossa:
3031303130312D393939582020202020

IV heksadesimaalimuodossa:
1457A63E941796F59DE04108938402A8

Avaimen binäärinen arvo esitettynä heksadesimaalimuodossa:
62C12760C2E68990DDD45FB77442161AAC39D454DB5A6454BAB599ACCE56C522

PMTREFNB-kentän salattu arvo heksadesimaalimuodossa:
1457A63E941796F59DE04108938402A8C335092F6D378CF934114772AF4DC905

5.3 Lisäselvitys USERMAC-parametrin käytöstä

Joissain tilanteissa saattaa esilläpitopalvelussa olla tarvetta verrata, onko verkkopankin käyttäjä sama kuin se, jolla on oikeus katsella tiettyjä tietoja tai tehdä jotain toimintoja.

Vertailu tehdään verkkopankin käyttäjän henkilötunnuksesta muodostetun tarkisteen USERMAC avulla.

USERMAC muodostetaan koko linkin tarkisteen tapaan (ks. 5.6.1 ja 5.7.1) seuraavasti:

- Muodostetaan merkkijono aikaleimasta, henkilötunnuksesta ja avaimesta &-merkillä eroteltuina, esimerkiksi TIMESTMP&HENKILÖTUNNUS&AVAIN&
- Henkilötunnuksessa on merkkijonossa mukana välimerkki ja mahdollinen kirjain on suuraakkosella.
- Tälle merkkijonolle lasketaan ALG-kentän mukaisella algoritmilla tiivistearvo, joka sijoitetaan kentän USERMAC arvoksi heksadesimaalimuodossa suuraakkosilla esitettynä.

Jos esilläpitopalvelussa on rekisteröitynä niiden henkilöiden tunnukset, jotka saavat selailla tiettyjä tietoja, voidaan oikeus tarkastaa muodostamalla vastaava merkkijono laskuttajan tiedoista, laskemalla siitä tarkiste ja vertaamalla näin saatua tarkistetta parametrikenttään USERMAC.

HUOM: Tarkastus edellyttää, että esilläpitopalvelun tarjoajan järjestelmässä on rekisteröitynä henkilötunnukset, sillä henkilötunnusta ei välitetä verkkopankkilinkissä selkokielisenä.

Jos USERMAC-avaimen muodostamiseen käytetty salainen avain on tiedossa, parametria USERMAC ei tulisi ajatella riittävänä suojakeinona, mikäli tavoitteena on suojata käyttäjän henkilötunnusta paljastumiselta. Tämä on syytä huomioida, kun verkkopankkilinkin sisältöä tarkastellaan tietosuojan näkökulmasta.

5.4 Lisäselvitys KEYVERS -parametrin käytöstä

KEYVERS-parametrilla ilmaistaan verkkopankkilinkin MAC-tarkisteen sekä USERMAC-kentän sisältämän tarkisteen laskennassa käytettävän salaisen avaimen versionumero. Versionumero koostuu arvoista välillä 0000-9999. Versionumero kasvaa aikajärjestyksessä, niin että vanhimmalla versiolla on pienin versionumero.

Avain tulee päivittää uuteen, mikäli on syytä epäillä sen olevan kolmannen osapuolen tiedossa. Kumpikin osapuoli on velvollinen pyytämään avaimen vaihtoa, jos on syytä epäillä, että avain on päätynyt ulkopuolisen tietoon.

Kun esilläpitopalvelussa on avattu ensimmäisen kerran validi linkki uudella avaimen versionumerolla, tulee esilläpitopalvelun hylätä kaikki pyynnöt, jotka sisältävät tätä versiota pienemmän versionumeron ja TIMESTMP arvon, joka on kyseisen uudella versionumerolla avatun linkin TIMESTMP arvoa myöhäisempi. Kyseisessä tilanteessa on aina kyse väärinkäytöksestä, jossa kolmas osapuoli käyttää haltuunsa saamaansa avainta luodakseen oikeudettomasti mielivaltaisia linkkejä.

Vastaavasti otettuaan käyttöön uuden avaimen pankki ei saa enää muodostaa uusia verkkopankkilinkkejä, jotka sisältävät vanhalla avaimella allekirjoitetun MAC- tai USERMAC-tarkisteen, ellei ole käynyt selväksi, että uudella avaimella luodut linkit eivät toimi esilläpitopalvelussa. Pankin ei tule normaalikäytössä, ilman pakottavaa syytä, ottaa uutta avainta käyttöön, ennen kuin se on otettu käyttöön esilläpitopalvelussa.

Kun osapuolet ovat vaihtaneet keskenään uuden salaisen avaimen, tulee vanhan avaimen voimassaolon lakata viimeistään 24 tunnin kuluttua tästä hetkestä. Tämän jälkeen esilläpitopalvelun tulee hylätä kaikki linkit, jotka on muodostettu vanhalla avaimella. Samoin pankki ei saa enää tämän jälkeen muodostaa uusia verkkopankkilinkkejä, jotka sisältävät vanhalla avaimella allekirjoitetun MAC- tai USERMAC-tarkisteen.

5.5 Lisäselvitys ENCKEYVER -parametrin käytöstä

ENCKEYVER-parametrilla ilmaistaan PMTREFNB-kentän salauksessa käytettävän salausavaimen versionumero. Versionumero koostuu arvoista välillä 0000-9999. Versionumero kasvaa aikajärjestyksessä, niin että vanhimmalla versiolla on pienin versionumero.

Avain tulee päivittää uuteen, mikäli on syytä epäillä sen olevan kolmannen osapuolen tiedossa. Kumpikin osapuoli on velvollinen pyytämään avaimen vaihtoa, jos on syytä epäillä, että avain on päätynyt ulkopuolisen tietoon.

Kun osapuolet ovat vaihtaneet keskenään uuden salausavaimen, tulee vanhan avaimen voimassaolon lakata viimeistään 24 tunnin kuluttua tästä hetkestä. Tämän jälkeen esilläpitopalvelun tulee hylätä kaikki linkit, jotka on muodostettu vanhalla avaimella. Samoin pankki ei saa enää tämän jälkeen muodostaa uusia verkkopankkilinkkejä, jotka sisältävät vanhalla avaimella salattua materiaalia.

5.6 Kuluttajan e-laskuun muodostettava linkki

Verkkopankissa linkki muodostetaan pankkikohtaisten sääntöjen mukaisesti e-laskuna toimitettuun maksuun, jota verkkopankin asiakas katsoo omassa verkkopankissaan.

Linkin parametrien sisältämien tietojen avulla linkki voidaan kohdistaa laskujen esilläpitopalvelussa oikeaan laskuun.

Linkin parametrien osalta on huomioitava:

- SENDID:nä käytetään pankin BIC-tunnusta
- PMTREFNB-kentässä on kuluttajan e-laskussa laskuun liittyvän lisätiedon arkistointitunnus (esimerkiksi laskun viite, laskuttaja syöttää tiedon Finvoice-laskulle kenttään InvoiceUrlText).
- parametri RCVID ei ole käytössä

Ennen linkin hyväksymistä sen sisältämät parametrikentät ja niiden arvot tulee validoida seuraavien ehtojen mukaisesti. Mikäli jokainen ehto ei täyty, tulee linkki hylätä.

1. linkin täytyy sisältää jokainen alla listattu pakollinen parametri
2. kunkin pakollisen parametrin tulee sisältyä linkkiin tasan yhden kerran
3. kunkin valinnaisen parametrin tulee sisältyä linkkiin korkeintaan yhden kerran
4. linkki ei saa sisältää mitään muita parametreja, kuin alla määritellyt pakolliset ja valinnaiset parametrit
5. kunkin parametrin tulee sisältää vain määriteltyjä merkkejä
6. kunkin parametrin tulee sisältää vain määritellyn lukumäärän verran merkkejä
7. yhdenkään parametrin arvo ei saa sisältää merkkejä ’=’ tai ’&’

Linkkiin sisältyvät pakolliset parametrit:

- VERSION
- PMTREFNB
- TIMESTMP
- KEYVERS
- ALG
- LANGCODE

- SESSIONID
- SENDID
- STATUS
- MAC

Linkkiin sisältyvät valinnaiset parametrit:

- PMTORIG
- ENCALG
- ENCKEYVER
- USERMAC

Esimerkki:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMTREFNB=12345678901 234567890&TIMESTMP=2021-11-16-102030%2B02&KEYVERS=0001&ALG=0003&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&ENCALG=0001&ENCKEYVER=0001&USERMAC=1234567890123456789012345678901 2&MAC=A62B3A510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2E6626

5.6.1 Kuluttajan e-laskun MAC-tarkisteen laskeminen:

MAC-laskennassa käytettävä merkkijono muodostuu parametrikenttien sisällöistä ja &-merkeistä seuraavasti:

VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&

Parametrikentät sijoitetaan merkkijonoon aina samassa järjestyksessä. Mikäli jokin valinnainen parametri ei ole mukana linkissä, käytetään sen tilalla tyhjää eli nollan merkin pituista arvoa.

Merkkijonon loppuun liitetään MAC-avain ja &-merkki. Merkkijonot eivät sisällä tyhjemerkkejä. Lopputulos on:

VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&MAC&

Mahdollinen URL-enkoodaus tulee purkaa parametreistä ennen MAC-tarkisteen laskemista.

Tälle merkkijonolle lasketaan ALG-kentän mukaisella algoritmilla tiivistearvo, joka sijoitetaan heksadesimaalimuodossa, suuraakkosina esitettynä, parametrikentän MAC-arvoksi. **HUOM!** MAC-arvon mahdolliset pienaakkoset muutetaan suuraakkosiksi.

Esimerkki:

Esimerkkilinkki:
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMTREFNB=12345678901 234567890&TIMESTMP=2021-11-16-102030%2B02&KEYVERS=0001&ALG=0003&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&ENCALG=0001&ENCKEYVER=0001&USERMAC=12345678901234567890123456789012&MAC=A62B3A510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2E6626

esimerkissä käytetyn MAC-avaimen binäärinen arvo heksadesimaalisessa tekstimuodossa:

A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E4F7DC

Koko merkkijono, josta esimerkin tiivistearvo lasketaan, esitettynä tekstimuodossa:

0020&12345678901234567890&2021-11-16-102030+02&0001&0003&1&12345&Prod&NDEAFIHH&1&0001&0001&12345678901234567890123456789012&A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E4F7DC&

HUOM! Kentän TIMESTMP enkoodaus on laskennassa muutettu takaisin +-merkiksi:

2021-11-16-102030%2B02 on laskennassa siis muodossa 2021-11-16-102030+02

Koko merkkijono, josta tiivistearvo lasketaan, esitettynä heksadesimaalimuodossa:

303032302631323334353637383930313233343536373839302632303231 2D31312D31362D3130323033302B3032263030303126303030333263126313233343526507264F64264E4445414649484826312630303031263030303126313233343536373839303132333435363738393031323334353637383930313233343536373839303132264133444432334636363131463931383542394130304136414446314445433032333737354444304238363041453930323937314332443036453145344637444326

Tiivistearvo:

A62B3A510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2E6626

5.7 Verkkopankkiin muodostettava linkki

Tässä tarkoitetaan linkkiä, josta pääsee esimerkiksi verkkopalkkapalveluun.

Ennen linkin hyväksymistä sen sisältämät parametrikentät ja niiden arvot tulee validoida seuraavien ehtojen mukaisesti. Mikäli jokainen ehto ei täyty, tulee linkki hylätä.

1. linkin täytyy sisältää jokainen alla listattu pakollinen parametri

2. kunkin pakollisen parametrin tulee sisältyä linkkiin tasan yhden kerran
3. kunkin valinnaisen parametrin tulee sisältyä linkkiin korkeintaan yhden kerran
4. linkki ei saa sisältää mitään muita parametreja, kuin alla määritellyt pakolliset ja valinnaiset parametrit
5. kunkin parametrin tulee sisältää vain määriteltyjä merkkejä
6. kunkin parametrin tulee sisältää vain määritellyn lukumäärän verran merkkejä
7. yhdenkään parametrin arvo ei saa sisältää merkkejä ’=’ tai ’&’

Linkkiin sisältyvät pakolliset parametrit:

- VERSION
- PMTREFNB
- RCVID
- TIMESTMP
- KEYVERS
- ALG
- LANGCODE
- SESSIONID
- SENDID
- STATUS
- MAC

Linkkiin sisältyvät valinnaiset parametrit:

- PMTORIG
- ENCALG
- ENCKEYVER
- USERMAC

Esimerkki:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMTREFNB=3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BEE651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&RCVID=12345678&TIMESTMP=2021-11-16-102030+02&KEYVERS=0001&ALG=0004&MAC=FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84039CDBD439&LANGCODE=1&SESSIONID=12345678901234567890&SENDID=PLACEHOLDER&STATUS=Prod&PMTORIG=1&USERMAC=12345678901234567890123456789012&ENCALG=0001&ENCKEYVER=0001

5.7.1 Verkkopankkilinkin MAC-tarkisteen laskeminen:

MAC-laskennassa käytettävä merkkijono muodostuu parametrikenttien sisällöistä ja &-merkeistä seuraavasti:

VERSION&PMTREFNB&RCVID&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&

Parametrikentät sijoitetaan merkkijonoon aina samassa järjestyksessä. Mikäli jokin valinnainen parametri ei ole mukana linkissä, käytetään sen tilalla tyhjää eli nollan merkin pituista arvoa.

Merkkijonon loppuun liitetään MAC-avain ja &-merkki. Merkkijonot eivät sisällä tyhjemerkkejä. Lopputulos on:

VERSION&PMTREFNB&RCVID&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&MAC&

Mahdollinen URL-enkoodaus tulee purkaa parametreistä ennen MAC-tarkisteen laskemista.

Tälle merkkijonolle lasketaan ALG-kentän mukaisella algoritmilla tiivistearvo, joka sijoitetaan heksadesimaalisina suuraakkosina parametrikentän MAC-arvoksi. HUOM! MAC-arvon mahdolliset pienaakkoset muutetaan suuraakkosiksi.

Esimerkki:

Esimerkkilinkki:
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMTREFNB=3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BEE651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&RCVID=12345678&TIMESTMP=2021-11-16-102030+02&KEYVERS=0001&ALG=0004&MAC=FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84039CDBD439&LANGCODE=1&SESSIONID=12345678901234567890&SENDID=PLACEHOLDER&STATUS=Prod&PMTORIG=1&USERMAC=12345678901234567890123456789012&ENCALG=0001&ENCKEYVER=0001

esimerkissä käytetyn MAC-avaimen binäärinen arvo heksadesimaalisessa tekstimuodossa:

A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E4F7DC

Koko merkkijono, josta esimerkin tiivistearvo lasketaan, esitettynä tekstimuodossa:

0020&3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BEE651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&12345678&2021-11-16-102030+02&0001&0004&1&12345678901234567890&Prod&PLACEHOLDER&1&0001&0001&12345678901234567890123456789012&A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E4F7DC&

HUOM! Kentän TIMESTMP enkoodaus on laskennassa muutettu takaisin +-merkiksi:

2021-11-16-102030%2B02 on laskennassa siis muodossa 2021-11-16-102030+02

Koko merkkijono, josta tiivistearvo lasketaan, esitettynä heksadesimaalimuodossa:

303032302633444632383142414138423832443238414642384537414435333143333638333532383044433345433936353036354238413442454536353145343139394142364645313442443244334246463339333143454639364230433244363131354326313233343536373826323032312D31312D31362D3130323033302B3032263030303126303030342631263132333435363738393031323334353637383930265072 6F6426504C414345484F4C4445522631263030303126303030312631323334353637383930313233343536373839303132333435363738393031323334353637383930313226413344443233463636313146393138354239413030413641444631444543303233373735444430423836304145393032393731433244303645314534463744432 6

Tiivistearvo:

FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84039CDBD439